93 年第 3 季偵測弱點之說明與修補方式

一. W32/Sasser

1. 簡要說明：

W32/Sasser 是隻針對 Windows Local Security Authority Service Server (LSASS)緩衝區溢位弱點所攻擊的網蟲。W32/Sasser 會隨機挑選 IP 位址，試著去掃描主機是否爲開啓 port 445 的 windows 平台，探測主機是否存在 LSASS 的弱點，若有則進行感染散播。而尚未修補弱點的主機會在網蟲探測感染後，會導致 LSASS.exe 程序執行異常，Windows 會顯示一分鐘後關機的警訊。

2. 受影響平台：

Windows NT

Windows 2000

Windows 2003

3. 檢測方式：

3.1 檢查主機是否已遭 W32/Sasser 感染

W32/Sasser 爲了每次開機都會自動被執行，他會在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 加入一登錄值，avserve.exe。若有此登錄值，表示該主機已遭 W32/Sasser 感染。

3.2 檢查主機是否有 LSASS 弱點

檢查主機是否存在 LSASS 弱點，可用 Nuessus 做外部掃描，掃描的 plugin ID 爲 12209。

4. 弱點修正：

4.1 若已遭 W32/Sasser 感染

若經上述的檢測方式確定主機已遭 W32/Sasser 感染，請至 Symantec 下載病毒移除工具 FxSasser.exe，下載網址，http://securityresponse.symantec.com/avcenter/FxSasser.exe，病毒移除工具的使用方式請參考 Symantec 的說明文件，http://www.symantec.com/region/tw/techsupp/avcenter/venc/data/tw-w32.sasser.removal.tool.html。

4.2 修補 LSASS 弱點

LSASS 的弱點已在微軟的安全性公告 MS04-011(http://www.microsoft.com/taiwan/security/bulletins/ms04-011.asp)有相關描述，微軟也提供修補程式，在 MS04-011 有提供下載的連結，請使用者根據自己作業系統的版本與語系下載適合的修補程式安裝，或是使用 Windows Update 進行更新。MS04-011 除了修正 LSASS 弱點外，還修正了其他微軟作業系統平台的安全性問題，詳細資料請參閱 MS04-011。

5. 參考資料：

Microsoft 安全性公告 MS04-011

http://www.microsoft.com/taiwan/security/bulletins/ms04-011.asp

Sasser 蠕蟲的常見問題集

http://www.microsoft.com/taiwan/security/incident/sasserfaq.asp

Symantec 安全威脅 - W32.Sasser.Worm

http://www.symantec.com/region/tw/techsupp/avcenter/venc/data/tw-w32.sasser.worm.html

Symantec - W32.Sasser 移除工具

http://www.symantec.com/region/tw/techsupp/avcenter/venc/data/tw-w32.sasser.removal.tool.html

二.Microsoft SQL Hello Overflow

1. 簡要說明：

在 Microsoft SQL Server 7.0 版本 7.00.1077 之前與 Microsoft SQL Server 2000 版本 8.00.760 之前存在著某些弱點，這弱點在客戶端向 Microsoft SQL server 進行連線時，如果客戶端傳送特殊的訊息，可能會造成 Microsoft SQL Server 執行發生問題，進而取得系統的控制權。若您的 SQL Server 7.0 版本高於 7.00.1077，或 SQL Server 2000 版本高於 8.00.760，但仍收到弱點修補通知，請與技服中心聯絡。版本查詢方法請參閱下方第三項：檢測方式。

2. 受影響平台：

Microsoft SQL Server 7.0

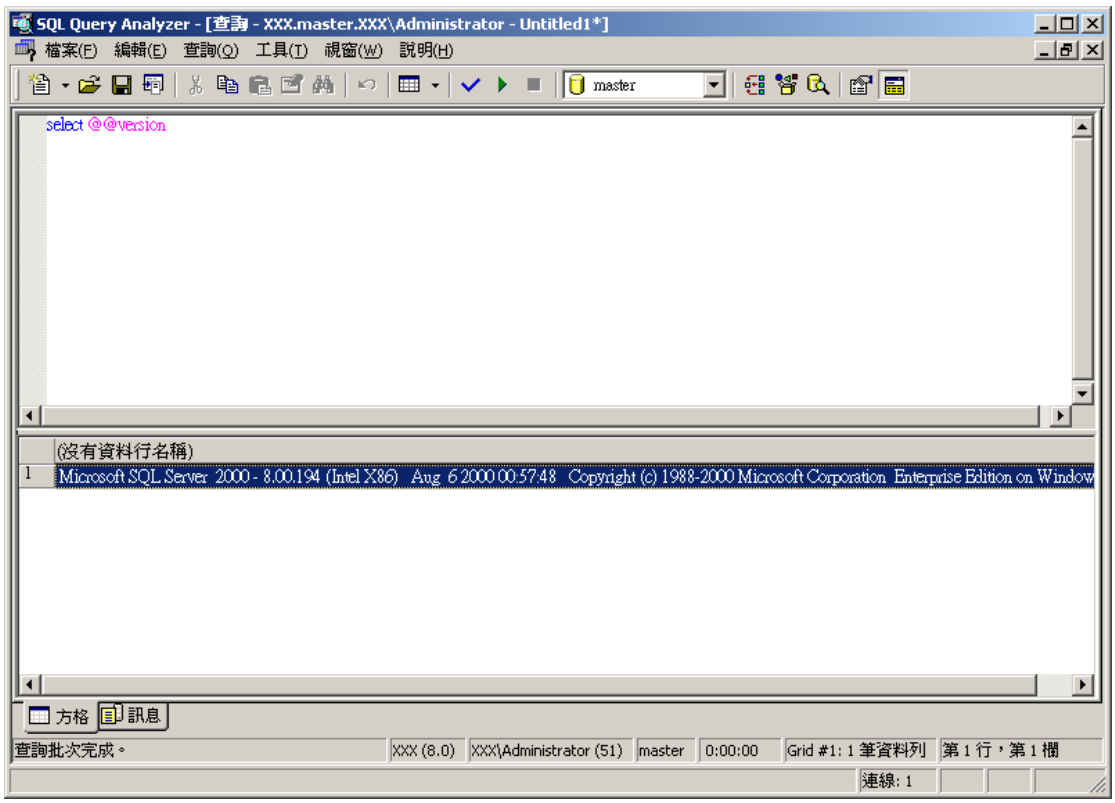
Microsoft SQL Server 2000

Microsoft Data Engine (MSDE) 1.0

Microsoft Desktop Engine (MSDE) 2000

3. 檢測方式：

檢查 Microsoft SQL Server 版本，Microsoft SQL Server 7.0 的版本比 7.00.1077 舊，與 Microsoft SQL Server 2000 的版本比 8.00.760 舊，皆會受到這個弱點的影響。使用者可以在 Microsoft SQL Server 所提供的 SQL Query Analyzer 執行"select @@version"，查詢所使用 Microsoft SQL Server 的版本，如下圖所示，



4. 弱點修正：

請下載並安裝 Microsoft SQL Server 最新修補程式。

4.1 Microsoft SQL Server 7.0

Microsoft SQL Server 7.0 的最新修補程式在下面網址，http://www.microsoft.com/downloads/details.aspx?FamilyId=FE5B0892-A5C9-44C2-9B42-0D291E9C1636&displaylang=en，安裝最新的修補程式前，系統需先安裝下列修補程式，Microsoft SQL Server 7.0 SP4 與 Microsoft Windows 2000 SP1，請按照下述順序安裝

(1) Microsoft Windows 2000 SP1(因爲測試的平台爲 Microsoft Windows 2000，若使用者使用其他的 Windows 作業系統，可能會需要先將系統升級到某個版本 Service Pack，強烈建議爲系統安裝最新的修補程式，如目前 Windows 2000 最新的 Server Pack 是 SP4)，請參考
http://www.microsoft.com/taiwan/windows2000/downloads/servicepacks/default.htm

(2) Microsoft SQL Server 7.0 SP4，請參考
http://www.microsoft.com/sql/downloads/sp4.asp

(3) Microsoft SQL Server 7.0 最新累積修補程式，請參考
http://www.microsoft.com/downloads/details.aspx?FamilyId=FE5B0892-A5C9-44C2-9B42-0D291E9C1636&displaylang=en

4.2 Microsoft SQL Server 2000

Microsoft SQL Server 2000 的最新修補程式爲 Microsoft SQL Server 2000 SP3a，http://www.microsoft.com/taiwan/sql/downloads/2000/sp3.htm，安裝此 SQL Server Service Pack 前需先安裝 Microsoft Windows 2000 SP1，請按照下述順序安裝

(1) Microsoft Windows 2000 SP1(同 Microsoft SQL Server 7.0 所述)

(2) Microsoft SQL Server 2000 SP3a，請參考
http://www.microsoft.com/taiwan/sql/downloads/2000/sp3.htm

Microsoft SQL Server 2000 將自己的 service pack 分成 3 個部分，

Sql2ksp3.exe，資料庫元件的更新

Sql2kasp3.exe，Analysis Services 元件的更新

Sql2kdesksp3.exe，Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) 的更新

請依照自己當初安裝 Microsoft SQL Server 所選元件安裝適當的修補程式，一般來說安裝 Sql2ksp3.exe 即可。

5. 參考資料：

Microsoft Security Bulletin MS02-056

http://www.microsoft.com/technet/security/bulletin/MS02-056.mspx

Microsoft Security Bulletin MS02-061

http://www.microsoft.com/technet/security/bulletin/ms02-061.mspx

Service Packs for Microsoft SQL Server

http://www.microsoft.com/sql/downloads/servicepacks.asp

三.Microsoft Exchange extended verb Buffer Overflow

1. 簡要說明：

在某些版本 Microsoft Exchange 的 extended verb 實作時出現問題，extended verb 提供 SMTP 延伸的功能，懷有惡意的人可以對未修補的 Microsoft Exchange 5.0 或 5.5 進行阻斷式服務攻擊，或是取得未修補的 Microsoft Exchange 2000 管理權。Microsoft Exchange 2003 並無這個弱點問題。

2. 受影響平台：

Microsoft Exchange Server 5.0

Microsoft Exchange Server 5.5

Microsoft Exchange Server 2000

3. 檢測方式：

使用 Nessus 做檢查，此弱點的 plugin ID 爲 11889 - Exchange XEXCH50 Remote Buffer Overflow。

4. 弱點修正：

安裝 Windows Exchange Server 最新的修補程式。

4.1 Microsoft Exchange Server 2000

Microsoft Exchange Server 2000 的最新累積修補程式在下面網址，http://www.microsoft.com/downloads/details.aspx?FamilyID=43F5CDF6-D1E6-4476-B5F2-E17371236C3C&displaylang=en，安裝最新的修補程式前，系統需先安裝下列修補程式，Microsoft Exchange Server 2000 SP3 與 Microsoft Windows 2000 SP2，請按下述順序安裝，

(1) Microsoft Windows 2000 SP2(因爲測試的平台爲 Microsoft Windows 2000，若使用者使用其他的 Windows 作業系統，可能會需要先將系統升級到某個版本 Service Pack，強烈建議爲系統安裝最新的修補程式，如目前 Windows 2000 最新的 Server Pack 是 SP4)，請參考

http://www.microsoft.com/taiwan/windows2000/downloads/servicepacks/default.htm

(2) Microsoft Exchange 2000 Server SP3

http://www.microsoft.com/exchange/downloads/2000/sp3/default.asp

(3) Microsoft Exchange 2000 最新累積修補程式 - Update Rollup for Exchange 2000 (KB824282)

http://www.microsoft.com/downloads/details.aspx?FamilyId=E7AAA113-1403-4262-8269-4B2AB9AE5476&displaylang=en

4.2 Microsoft Exchange Server 5.5

Microsoft Exchange Server 5.5 的最新累積修補程式在下面網址，http://www.microsoft.com/downloads/details.aspx?FamilyID=6965FCA9-7C7D-40D6-9061-21F9903D398F&displaylang=en，安裝最新的修補程式前，系統需先安裝下列修補程式，Microsoft Exchange Server 5.5 SP4 與 Microsoft Windows 2000 SP2，請按下述順序安裝，

(1) Microsoft Windows 2000 SP2(同 Microsoft Exchange 2000 所述)

(2) Microsoft Exchange Server 5.5 SP4

http://www.microsoft.com/exchange/downloads/55/sp4.asp

(3) Microsoft Exchange 5.5 最新累積修補程式 - Update Rollup for Exchange 5.5(KB841765)

http://www.microsoft.com/downloads/details.aspx?FamilyID=6965FCA9-7C7D-40D6-9061-21F9903D398F&displaylang=en

(4) Security Update for Exchange 5.5 (KB829436)

http://www.microsoft.com/downloads/details.aspx?FamilyID=A9E872EA-54B0-4179-8AE9-5648BFB46459&displaylang=en

4.3 Microsoft Exchange Server 5

Microsoft Exchange Server 5 的最新累積修補程式在下面網址，http://www.microsoft.com/downloads/details.aspx?FamilyId=164610A4-AAFC-40AC-85CA-349DBDBE1731&displaylang=en，安裝最新的修補程式前，系統需先安裝下列修補程式，Microsoft Exchange Server 5 SP2 與 Microsoft Windows 2000 SP2，請按下述順序安裝，

(1) Microsoft Windows 2000 SP2(同 Microsoft Exchange 2000 所述)

(2) Microsoft Exchange Server 5 SP2

http://support.microsoft.com/default.aspx?kbid=168858

(3) Update Rollup for Exchange 5(KB834130)

http://www.microsoft.com/downloads/details.aspx?FamilyId=164610A4-AAFC-40AC-85CA-349DBDBE1731&displaylang=en

5. 參考資料：

Microsoft Security Bulletin MS03-046

http://www.microsoft.com/technet/security/bulletin/MS03-046.mspx

四.Microsoft IIS .HTR overflow

1. 簡要說明：

HTR 是一種類似 ASP 的網頁程式，在 IIS 2.0 的時代就已經出現了，比 ASP 還要早出現，但是 HTR 很少被應用，因爲他的功能幾乎被 ASP 所取代，但即使如此，一直到 Microsoft IIS 5.0 還是有支援 HTR。負責處理 HTR 的 ISAPI extension 被發現有弱點，懷有惡意的人可以利用這弱點對有缺陷的系統進行阻斷服務式攻擊或是取得系統的控制權。

2. 受影響平台：

Microsoft IIS 4.0

Microsoft IIS 5.0

3. 檢測方式：

檢查 ism.dll 的版本，ism.dll 的預設路徑爲 C:\WINNT\System32\inetsrv\ism.dll，這個路徑可能會因安裝設定的不同而有所不同，若 ism.dll 的版本舊於 5.00.2195.5671 的話，表示該系統可能會受到這弱點的影響，管理者應立即進行修補。

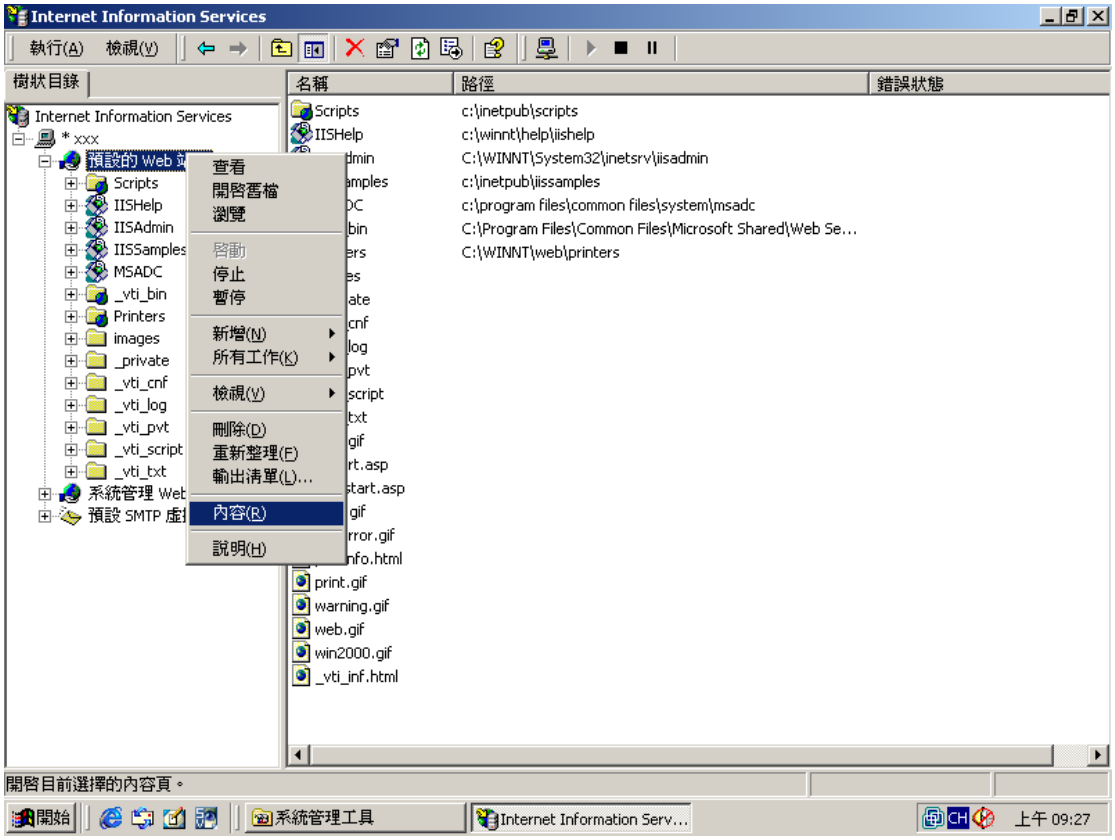
4. 弱點修正：

4.1 移除 Microsoft IIS 對.HTR 的支援

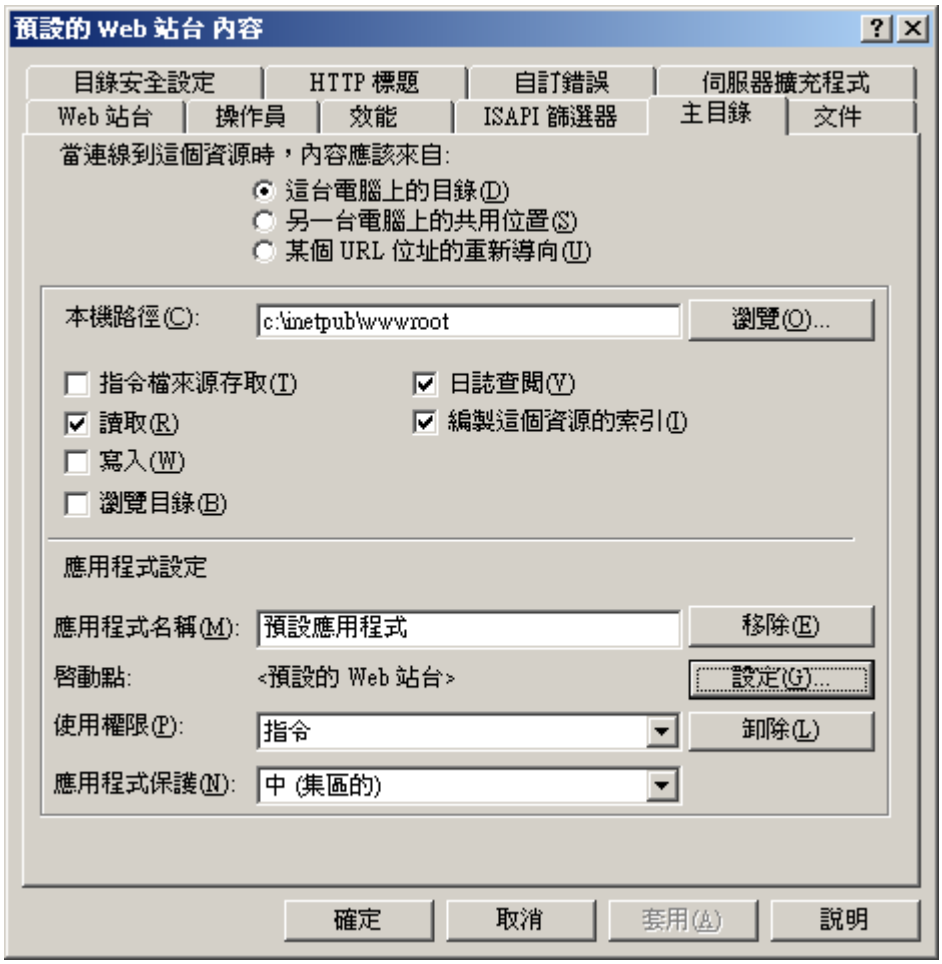
若管理者確定網站沒有應用.HTR 的話，建議直接移除 Microsoft IIS 對.HTR 的支援，以 Microsoft IIS 5.0 爲例，移除的步驟如下，

(1) 打開 Internet 服務管理員

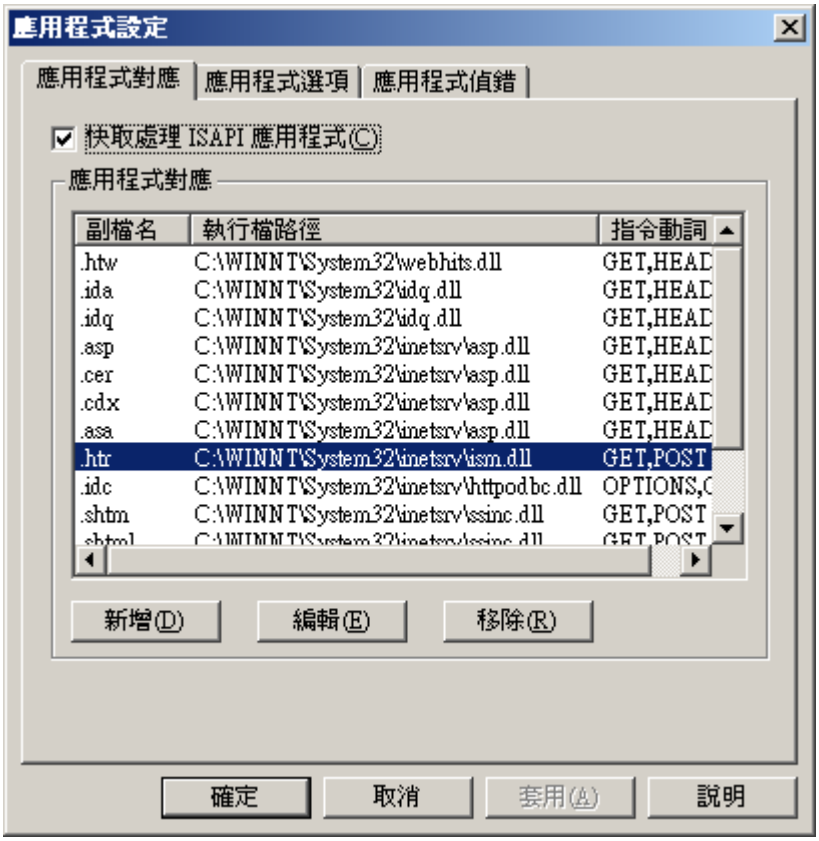
Internet 服務管理員的路徑爲，開始->設定->控制台->系統管理工具，其畫面如下，



(2) 選擇 web 站台，預設名稱爲"預設的 Web 站台"，在上面點選滑鼠右鍵，選擇內容，並選擇"主目錄"，會出現下面的畫面，


預設的 Web 站台 內容
目錄安全設定
HTTP 標題
自訂錯誤
伺服器擴充程式
Web 站台
操作員
效能
ISAPI 篩選器
主目錄
文件
當連線到這個資源時，內容應該來自:
這台電腦上的目錄(D)
另一台電腦上的共用位置(S)
某個 URL 位址的重新導向(U)
本機路徑(C):
c:\inetpub\wwwroot
瀏覽(O)...
指令檔來源存取(T)
日誌查閱(V)
讀取(R)
編製這個資源的索引(I)
寫入(W)
瀏覽目錄(B)
應用程式設定
應用程式名稱(M):
預設應用程式
移除(E)
啓動點:
<預設的 Web 站台>
設定(G)...
使用權限(P):
指令
卸除(L)
應用程式保護(N):
中 (集區的)
確定
取消
套用(A)
說明

(3) 選擇"設定"，



(4) 在"設定"的"應用程式對應"可以找到副檔名爲.htr 的應用程式對應，點選它，並選擇下方的"移除"選項。

(5) 重新啓動 IIS。

4.2 安裝對.HTR 的最新修補程式

(1) windows 2000 上執行 IIS 5.0

下載並安裝 windows 2000 SP4，http://www.microsoft.com/taiwan/windows2000/downloads/servicepacks/sp4/，大部分的系統是屬於這種架構。

(2) Microsoft IIS 5.0

此弱點 IIS 5.0 的修補程式在 http://www.microsoft.com/windows2000/downloads/security/q321599/default.asp，請注意在安裝此修補程式時，會需要將 windows 作業系統升級到某個版本的 service pack，如在 windows 2000 下，需升級至 Windows 2000 SP1。

(3) Microsoft IIS 4.0

此弱點 IIS 4.0 的修補程式在 http://www.microsoft.com/ntserver/nts/downloads/security/q321599/default.asp，請選

擇適合的語系下載，請注意在安裝此修補程式時，會需要將 windows 作業系統升級到某個版本的 service pack。

5. 參考資料：

Microsoft Security Bulletin MS02-028

http://www.microsoft.com/technet/security/bulletin/MS02-028.mspx

五.修訂

2004-08-04：93 年第 3 季偵測弱點之說明與修補文件發佈

2004-08-31："Sassser 參考資料"連結更新

"SQL Hello Overflow 簡要說明"更新

"Exchange 弱點修正"更新